Business Email Compromise
Prevention Guide

Business Email Compromise (BEC)
typically involves a cybercriminal posing as an employee who can make payments or provide personally identifiable information (PII)—often a manager or executive—and sending emails to employees requesting funds to be transferred or confidential data provided, to waiting thieves or offshore accounts.

Common Attack Methods

Spear Phishing

Social Engineering

Email Spoofing

Malware

Statistics: By the Numbers

From October 2013 until June 2016, **BEC-related losses** were estimated at **$5.3 billion.**

In 2016, a single **BEC scammer** stole more than **$100 million** from a pair of U.S. corporations.

Three Common Types of BEC

There was a **480% increase** in the number of **BEC attacks** in 2016.

Fake Payment Request
Cybercriminal uses compromised account to send payment request to employee.

CEO Fraud
Cybercriminal poses as company executive and emails the finance department to request to send funds.

Data Theft
Cybercriminal uses compromised email to request PII of employees or executives.

Defend Yourself Against BEC
To defend yourself against BECs, follow these best practices:

Avoid replying to the sender, especially if this is being received from a personal email address. Instead, *forward your response* to the executive or manager's actual work email address.

Call the person who sent the request to *verify that it's legitimate.*

Double-check the email address of the sender to make sure it isn't being spoofed.

Be wary of changes in how the sender communicates, especially if you are asked to maintain secrecy or if the tone is urgent.

If you do fall victim to a BEC, it is very important to alert your manager quickly. If funds were transferred, there may be a chance to freeze the process and recover the funds.

WANT TO PROTECT YOURSELF & YOUR ORGANIZATION FROM BEC?

GO TO **INSPIREDELEARNING.COM/SECURITY-AWARENESS** TO LEARN HOW.